CLAIMS

1. Method for controlling access by a requestor (7) to resources (2d) in a computer system (1) in which the requester is assigned one or more roles based on an access control list that defines the conditions for obtaining a right to a resource, characterized in that it consists of restricting the resources accessible for a given role to only part of the resources, by means of a validity domain of the role.

2. Method according to claim 1, characterized in that it stores an additional piece of information relative to the need to consult the validity domain of the role in the access control list.

3. Method according to claim 2, characterized in that it consults the additional information relative to the need to consult the validity domain of the role and verifies that the resource in question belongs to the validity domain only if said information requires it.

4. Method according to claim 2, characterized in that it performs an access check on two levels:

- a first level on the type of the resource (2d);
- a second level on the identifier of the resource (2d).

5. Method according to claim 4, characterized in that it performs a first-level check verifying the existence of at least one entry of the access control list that satisfies the conditions for obtaining the requested right, and if the entry exists, the existence of a validity domain for said entry.

6. Method according to claim 5, characterized in that it performs a second-level check verifying, if the requested permission contains a resource identifier, the existence of at least one configured permission corresponding to the requested permission, and the value of the additional information relative to the need to consult the validity domain.

7. Method according to any of claims 1 through 5, characterized in that it consists of grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

8. Device for controlling access by a requestor to resources (2d) in a computer system (1), characterized in that it comprises a management machine (2a) comprising an access control service, the RAC (6), and means for storing (10) roles, access control lists and validity domains

9. Device for implementing the method according to any of claims 1 through 6.

10. Software module for implementing the method according to any of claims 1 through 6.